

SUBJECT:	INFORMATION GOVERNANCE UPDATE
DIRECTORATE:	CHIEF EXECUTIVE AND TOWN CLERK
REPORT AUTHOR:	SALLY BROOKS, DATA PROTECTION OFFICER (DPO)

1. Purpose of Report

- 1.1. To update Committee on the Council's Information Governance compliance and associated risks. This includes compliance with the Data Protection Legislation including the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA).
- 1.2. This report also includes monitoring of the Council's compliance with its legal obligations under the Freedom of Information Act 2000.

2. Background of Reporting

- 2.1. Reports are submitted biannually to Committee and in line with reports submitted to Corporate Leadership Team (IG Board). The last report provided to Committee was 10 December 2024.

3. Information Governance (IG) Risk Register

- 3.1 See Appendix A (Part B) for the Council's Information Governance Risk Register. All risks require continuous mitigation and monitoring to ensure current Assurance Levels are maintained or improved.
- 3.2 The following risks are highlighted for comment in this report:
 - Training
 - Policies, and Procedures (including legislation reform)
 - Retention and Disposal of Personal Data
 - Data Subject's Rights and Freedom of Information Requests

4 Training (Risk 1)

- 4.1 Data protection training is an organisational security measure required for compliance with the Data Protection Legislation. Training is provided on induction for new staff/members and annually. Additional training is provided to Service Managers who are Information Asset Owners (IAO's) and responsible for personal data in their service areas.
- 4.2 The current online training package 'Cyber Ninjas' is produced in association with the National Cyber Security Centre (NCSC) and covers both data protection and cyber security.
- 4.3 When the Council are required to report a data breach to the regulator the Information Commissioner's Office (ICO), they must confirm those staff/members involved have received data protection training in the last 2 years.
- 4.4 Final training completion rates for 2024 are at 92% for all staff. Those who did not complete this must complete both last year's full course and this year's refresh course.

The importance of completing this mandatory training is being reinforced through IAO's, Assistant Directors and the Council's Senior Information Risk Officer (SIRO).

- 4.5 This year's annual refresh of training was deployed on the 04 March 2025. This is a quick refresh of last year's full course which tests knowledge with a quiz, and which must be passed before completion is recorded centrally. Staff have been requested to complete this by 01 July 2025.
- 4.6 Members will be offered a face-to-face refresh of training later this year to be arranged with democratic services. This is in addition to the option for members to complete the bespoke Councillor Cyber Ninja's training online.
- 4.7 The Council have a dedicated Data Protection Hub site for staff and members and an IAO Microsoft Teams Channel. These provide regular data protection and cyber security related news posts, templates, handbook, policies and guidance. Also links to further training including the ICO's own Freedom of Information staff training videos.
- 4.8 The Council continue with their communications campaign 'Think before you click'. This includes the release of articles/video clips regarding cyber security and data protection. Also, posters displayed around the Council's offices with key messages to staff/members on how to protect personal data.

5. Policies and Procedures (Risk 3) proposed legislation reform

- 5.1 A review of Information Governance policies has been delayed to September 2025 due to the forthcoming data protection legislation reform (likely to come into force before the end of this parliamentary session in July 2025). This is the [Data \(Use and Access\) Bill](#) currently in the final stages of being considered by Parliament and a briefing note will be provided Audit Committee once amendments have been considered and the Bill receives approval.
- 5.2 There are likely to be a number of changes in the new reform legislation which will amend the existing Data Protection Legislation (including UK GDPR and the Data Protection Act 2018) which will need to be reflected in the Council's Information Governance policies and procedures. For example, the likely mandating of a complaints procedure for Data Subject Access Requests, where currently the Council inform of the right to complain to the independent regulator the Information Commissioner's Office (ICO).
- 5.3 Microsoft 'Copilot' is available to staff as an application in their web browser. This is not currently approved for use by staff/members. An acceptable usage Artificial Intelligence (AI) policy has been drafted and will be considered for approval shortly.
- 5.4 AI has potential benefits for the Council such as improvements in productivity, efficiency and outcomes for customers. However, risks of AI must be considered and mitigated from the outset. This is a fast-developing area which requires strategic planning by the Council. Currently access to all other forms of AI via the Council's network have been removed whilst this is considered.
- 5.5 Internal Audit will be carrying out an Audit of Information Governance processes and procedures as part of their Audit Plan for 2025-26. Audit and self-assessment are an essential aspect of demonstrating the Council's Information Governance compliance.

6. Retention and Disposal of Personal Data (Risk 5)

- 6.1 An analysis of the electronic data held by the Council is currently ongoing as part of the IT migration project. This has begun with an analysis of data held over 6 years and which is being provided to IAO's to review for deletion before data is migrated.
- 6.2 Retention policies must be automated from the outset on data migrated and on existing data already held in the Cloud such as in Office 365, SharePoint and Microsoft Teams as soon as possible.
- 6.3 A retention period of 6 months has been agreed to be implemented on Microsoft Teams 1-1 Chat. This was with a 3 month lead up to implementation to allow staff/members time to review any data to be retained. Communications have been deployed to inform all staff/members of this, and automated deletion will commence on 01 July 2025.

7. Data Subject's Rights (Risk 8)

- 7.1 Completion rates for Data Protection Act requests are detailed below by quarter since last reported. These include Data Subject Access Requests (DSARs) from individuals regarding their own personal data and requests for personal data from third parties such as the Police, NHS and Home Office.

Oct-Dec 2024	
Total requests received	41
Requests completed in time	88%
July-Sept 2024	
Total requests received	34
Requests completed in time	97%

- 7.2 By way of comparison, requests received, and completion rates previously reported:

Time periods	Requests received	Percentage completed in time:
April-June 2024	35	91%
Jan-March 2024	23	82%
Oct-Dec 2023	18	94%
July-Sept 2023	28	91%
April-June 2023	32	91%
Jan-March 2023	20	80%
Oct- Dec 2022	25	84%
July -Sept 2022	26	77%

- 7.3 The number of requests received by the Council continues to increase. The highest number ever recorded by the Council between October and December 2024 although these high numbers are not unusual and have been steadily increasing. In addition, requests are becoming increasing complex and resource intensive often relating to complaints, legal proceedings and HR matters.
- 7.4 DPA requests can be submitted by requesters through multiple channels such as e-form, email, letter, social media or even verbally. The Council can only encourage use of the online e-form. Current processes are largely manual, and the e-form system has its limitations. Therefore, the Council continues to explore options for improvements to existing processes.

8 Freedom of Information Requests

8.1 Response rates for requests under the Freedom of Information Act 2000 (FOI) are detailed below by quarter since last reported.

Jan-March 2025	
Total requests received:	207
Requests completed in time:	86%
Oct-Dec 2024	
Total requests received:	178
Requests completed in time:	87%
July-Sept 2024	
Total requests received	115
Requests completed in time	83%

8.2 By way of comparison, FOI requests received and completion in time percentage rates previously reported:

Time periods	Requests received	Percentage completed in time:
April-June 2024	181	86%
Jan-March 2024	179	85%
Oct-Dec 2023	206	87%
July-Sept 2023	200	89%
April-June 2023	174	86%
Jan-March 2023	205	89%
Oct- Dec 2022	95	61%
July -Sept 2022	75	54%

8.3 The number of FOI requests remains high. The highest number ever recorded by the Council between January and March 2025.

8.4 FOI rates have improved significantly in the last 3 years (due to improvements in internal processes). However, rates have plateaued in the last 2 years and are yet to reach 95% to be considered good by the Information Commissioner's Office (ICO). The Council are currently carrying out a detailed analysis of FOI requests received to establish if response rates can be improved, and numbers of requests reduced for example by proactively publishing more information.

8.5 FOI rates are published on the Council's website see link [key FOI statistics](#). The aim is to provide more detail in the line with ICO's guidance. This will be possible when automated reporting capabilities are available through improvements to existing processes which will also be considered as part of the current FOI analysis.

8.6 Internal Audit will be carrying out an Audit of FOI processes and procedures as part of Workplan Scheduling for 2025-26.

9. Annual Governance Statement (AGS)

9.1 Information Governance was removed from the AGS but remains closely monitored with reports biannually to IG Board (Corporate Leadership Team), and Audit Committee.

This is also monitored by an internal working group incorporating the Senior Information Risk Officer, Data Protection Officer, Audit, Legal, IT Managers and Comms Officer.

10. Strategic Priorities

10.1 This work ensures that staff and members are high performing in their collection and processing of customer and staff personal data. It also assists to ensure that the Council is 'trusted to deliver' services and compliant with the Data Protection Legislation.

11. Organisational Impacts

11.1 Finance (including whole life costs where applicable)

There are no financial implications arising from this report, as the resources will come from existing budgets.

11.2 Legal Implications including Procurement Rules

There are no legal implications arising out of this report.

11.3 Equality, Diversity and Human Rights

The Public Sector Equality Duty means that the Council must consider all individuals when carrying out their day-to-day work, in shaping policy, delivering services and in relation to their own employees.

It requires that public bodies have due regard to the need to:

- Eliminate discrimination.
- Advance equality of opportunity
- Foster good relations between different people when carrying out their activities.

There is no impact arising from this report regarding these issues.

12. Risk Implications

12.1 The Council must comply with the Data Protection Legislation. Non-compliance may result in enforced external audits, enforcement notices, monetary fines, criminal prosecutions of individual's, compensation claims and loss of public/partner trust. Non-compliance with the Freedom of Information Act 2000 may result in loss of public trust and enforcement action.

13. Recommendation

13.1 To note the content of the report including the IG register (Appendix A) and provide any comment.

Is this a key decision?	No
Do the exempt information categories apply?	No
Does Rule 15 of the Scrutiny Procedure Rules (call-in and urgency) apply?	No
How many appendices does the report contain?	One
List of Background Papers:	None
Lead Officer:	Sally Brooks, Data Protection Officer Email: sally.brooks@lincoln.gov.uk